UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/770,877 | 01/26/2001 | Jeffrey Bruce Lotspiech | ARC92001005US1 | 6667 |

7590 04/18/2005

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

| EXAMINER | |
|---|---|
| NGUYEN, MINH DIEU T | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

DATE MAILED: 04/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/770,877 | LOTSPIECH ET AL. | |
| | Examiner | Art Unit | |
| | Minh Dieu Nguyen | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *24 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-98* is/are pending in the application.

4a) Of the above claim(s) *44,62-64,68,82 and 89-94* is/are withdrawn from consideration.

5)☒ Claim(s) *65-67,69-81,83-88 and 97* is/are allowed.

6)☒ Claim(s) *1-6,8,10,11,19,21-26,28,30,31,39,41-43,45,46,48,50,51,61,95,96 and 98* is/are rejected.

7)☒ Claim(s) *7,9,12-18,20,27,29,32-38,40,47,49 and 52-60* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1. This action is in response to the amendment dated November 24, 2004.

### *Response to Arguments*

2. Applicant's arguments filed November 24, 2004 with respect to the rejection(s)of claim(s) 1, 21, 41, 61 and their dependent claims have been fully considered but they are not persuasive.

3. The applicant argues in substance the following: a) Schwenk does not teach partitioning users who are not in a revoked set into disjoint subsets having associated subset keys and b) there is no motivation to combine the teaching of Srivastava and Schwenk.

a) As to point a, the examiner relies upon Srivastava on teaching partitioning users into subgroups having associated subgroup keys (Fig. 5). Schwenk is merely relied upon on teaching the users on the revoked list should not be receiving the keys. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

b) As to point b, Schwenk discloses a method for securing a pay TV systems against unauthorized users (i.e. users in revoked group), while a system of Srivastava is

for creating a secure channel among the participating members (Abstract) to protect information against interception by an unauthorized party (i.e. users in revoked group; col. 1, lines 19-24; col. 2, line 58 to col. 3, line 3). Both, Srivastava and Schwenk references, relate to crypto keys and key revocation in secure network communication system.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-6, 8, 10-11, 19, 23-26, 28, 30-31, 39, 41-43, 45-46, 48, 50-51, 61, 95-96 and 98 are rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava, US Patent 6,684,331 in view of Schwenk, US Patent 6,222,923.

a) As to claims 1 and 41-42, Srivastava discloses a method and apparatus for distributing and updating group controllers or multicast service agents over a wide area network based on a tree structure comprising assigning each user in a group of users respective private information I.sub.u which reads on private key (Fig. 2A, elements A-H; col. 2, lines 17-18); selecting at least one session encryption key K (col. 2, lines 37-41); encrypting the session key K, which reads on group key GK, with the subset keys L.sub.i1 to L.sub.im to render m encrypted versions of the session key K (Fig. 5). Srivastava discloses Diffie-Hellman protocol in Fig. 5, where subset keys reads

on shared private key, however, it is well-known in the cryptography area that asymmetric algorithm is used to generate a ciphertext (col. 2, lines 1-8), wherein the sender encrypts the session key with the recipients public keys, which reads on the subset keys L.sub.i1 to L.sub.im. Srivastava teaches partitioning all users into disjoint subsets S.sub.i1 to S.sub.im having associated subset keys L.sub.i1 to L.sub.im, however Srivastava does not teach partitioning users not in a revoked set R into disjoint subsets.

Schwenk discloses a method of securing a pay TV system protected by a predefined hierarchy of cryptographic keys against unauthorized users comprising the step of partitioning users not in a revoked set into disjoint subsets (i.e. customers 1-4 with crypto keys PK1-PK4, correspondingly; Fig. 1, col. 3, lines 35-42).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of partitioning users not in a revoked set into disjoint subsets, as Schwenk teaches, in the system of Srivastava, so as to securely protect information with a better way of handling crypto keys for authorized users (non-revoked users) and unauthorized users (revoked users).

b) As to claims 2-3, 23 and 43, Srivastava discloses the method further comprising partitioning the users into groups S.sub.1 to S.sub.w, wherein "w" is an integer, and the groups establish subtrees in a tree wherein the tree is a complete binary tree (Fig. 5).

c) As to claims 4-5, 24-25, 45 and 98, Srivastava discloses the method further comprising using private information I.sub.u to decrypte the session key (col. 16,

lines 30-32). Srivastava discloses Diffie-Hellman protocol in Fig. 5, where subset keys reads on shared private key, however, it is well-known in the cryptography area that asymmetric algorithm is used to generate a ciphertext (col. 2, lines 1-8), wherein the sender encrypts the session key with the recipients public keys, which reads on the subset keys L.sub.i1 to L.sub.im. and the recipient decrypts the session key with the recipient's private key which reads on private information I.sub.u.

d) As to claims 6, 26 and 46, Srivastava discloses the method wherein each subset S.sub.i1 to S.sub.im includes all leaves in a subtree rooted at some node v.sub.i, at least each node in the subtree being associated with a respective subset key (Fig. 5, elements A-H, 507, 509, 511 and 513).

e) As to claims 8, 28 and 48, Srivastava discloses the method wherein each user must store log N keys, wherein N is the total number of users (col. 16, lines 17-19).

f) As to claims 10, 30 and 50, Srivastava discloses the method wherein the total number of users defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets. The revoked set R is a subset in the total number of users N, it is inherently understood that the same structure applied to the revoked set as well as to the total number of users.

g) As to claims 11, 31 and 51, Srivastava discloses the method wherein the tree includes a root (Fig. 5, element 501) and plural nodes (Fig. 5, elements 501, 503, 505, etc.), each node having at least one associated label (Fig. 5, elements 1, 2, etc.) and wherein each subset includes all leaves (Fig. 5, elements 11, A, B) in a subtree

rooted at some node v.sub.i (Fig. 5, element 503) that are not in the subtree rooted at some other node v.sub.j (Fig. 5, element 509) that descends from v.sub.i.

h) As to claims 19 and 39, Srivastava discloses the method wherein the tree includes a root and plural nodes, each node having an associated key, and wherein each user is assigned keys from all nodes in a direct path between a leaf representing the user and the root (Fig. 5).

i) As to claim 61, see the above addressed claims 1, 2 and 11.

l) As to claims 95 and 96, Swenk discloses the computer wherein the act of partitioning is undertaken by a system computer (Fig. 6).

6. Claims 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Srivastava, US Patent 6,684,331 in view of Schwenk, US Patent 6,222,923, in view of Hara, US 2004/0202328 and further in view of Akins, III et al. US Patent 6,560,340.

a) As to claim 21, Srivastava discloses a computer program device (Fig. 8) comprising a computer program storage device including a program of instruction usable by a computer comprising logic means for accessing a tree to identify plural subset keys; logic means for encrypting a message with a session key; logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key (Fig. 5). Srivastava and Schwenk do not teach logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers.

Hara discloses a data transmission system where data is transmitted to a plurality of receivers and the encrypted session key is sent to plural receivers (page 1,

paragraph [0014]; page 2, paragraphs [0018-0019]). Hara does not explicitly state the encrypted session key is in the header of the packet.

Akins explicitly discloses the encrypted session key is sent in a header of the message (col. 17, lines 66-67 to col. 18, lines 1-13; Fig. 10).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sending the encrypted session key in the message header to plural receivers, as Hara and Akins teach, in the system of Srivastava and Schwenk, so as to provide conditional access to data services (page 2, paragraph [0017]).

b) As to claim 22, this limitation is addressed above as part of claim 1.

### *Allowable Subject Matter*

7. Amended claims 65-67, 69-81, 83-88, and 97 are allowed.

8. Claims 7, 9, 12-18, 20, 27, 29, 32-38, 40, 47, 49, and 52-60 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### *Conclusion*

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
4/7/05

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER